International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 03 | Mar-2016 www.irjet.net p-ISSN: 2395-0072

A Comparative Survey of Various Cryptographic Techniques

Jitendra Singh Laser[1],Viny Jain[2]

[1]*M.E.(Communication Engineering) Scholar, SSTC, SSGI (FET),Bhilai (C.G.)India*

[2]*Associate Professor, SSTC,SSGI (FET),Bhilai(C.G.)India*

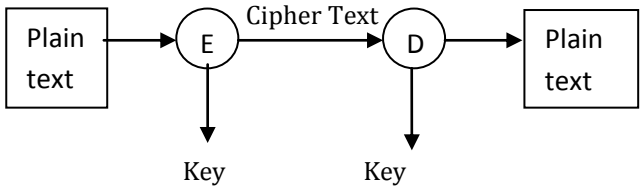
Abstract - *Now a days world that is characterized by the rapid rise in the number of attacking or hacking issues and more especially using more superior methods, it is prudent that a lot of IT research be intended for finding answer to the rising threats to the online or internet system , including the network itself and data and the information that carries and store from one location to another. Thus, information is a very important asset and must be kept confidential, have integrity and become available in order to be worth its name and be credible. The thought of information security lead to the development of Cryptography. In other words, Cryptography is the science of keeping information secure. It includes encryption and decryption of data or messages. Cryptography, in addition to providing confidentiality, also provides Integrity, Authentication and Non-repudiation. Based totally on the key distribution, cryptography is categorized into two important types-Symmetric Key Cryptography and Asymmetric Key Cryptography. In this paper, we've surveyed the conventional algorithms, based on their benefits and drawbacks. We additionally have in comparison the significance of each these cryptographic techniques. This paper also offer an appropriate future opportunity related to these cryptographic techniques.*

Key Words: *Man In The Middle Attack ; Biometric Sender Authentication; Diffie Hellman (DH) Key Exchange Algorithm; Speech and Message Encryption and Decryption;*

1.INTRODUCTION

In Cryptography is the art of science or collection of techniques or tools used to protect the data and information during its transmission over the network . It involves encryption and decryption of messages. Encryption is the process of converting a plain text into cipher text and decryption is the process of getting back the original message from the encrypted text. Cryptography, in addition to providing confidentiality, also provides Integrity, Authentication and Non-repudiation. The crux of cryptography lies in the key involved and the secrecy of the keys used to encrypt or decrypt. Cryptography contains various abstraction levels of security mechanism .Network administrator provides authorized access over the network by implementing network security and adoption of its provisions and policies to prevent unauthorized access. Authorization has always been an integral part of the security mechanism. Cryptography has played a important role in curbing down most information threats such as the man in the middle and eavesdropping attacks that target data and information as it moves over the internet system. However, research carried out by professionals in the field indicates that there could be some gaps that need to be filled in the area of cryptography so as to attain a better security of data and information.

1.1 Terms Used in Cryptography



E= Encryption , D= Decryption

Fig-1: General figure of cryptographic system

• *Plain Text* – The original message is used to communicate with the other is defined as plain text. E.g. A send " Hey "message to B. Here, " Hey "is a plain text message.

• *Cipher Text* - The non readableor meaningless message is called as cipher text. In cryptography, the original message is converted into non readable message. E.g. –"2J9" is a cipher text produced.

• *Encryption* - Encryption is a process of converting plain text into cipher text. Encryption techniques are used to send secret message by an insecure channel. Encryption process require an encryption algorithm and a key. Encryption takes place at the sender side.

• *Decryption*- Decryption is the reverse process of encryption where it converts text into plain text. Decryption takes place at receiver side to obtain the original message from meaningless message. Decryption process requires decryption algorithm and a key.

• *Key* – A key is a numeric or alpha numeric text. The key is used when encryption takes place on the plain text and at the time of decryption on the cipher text. In cryptography, selection of key is very important since the security of encryption algorithm depends on it.

1.2 Purpose of Cryptography

Cryptography provides a number of security aim to provide protection to information. Following are the aim of cryptography[1].

• *Confidentiality* – Ensures that transmitted information are accessible

only for reading by the authorized parties.

• *Authentication* – Ensures that origin of message is correctly identified, with an assurance that the identity is not false.

• *Integrity* – Ensures that only authorized parties are able to modify the transmitted information. Modification includes changing , writing ,deleting of transmitted.

Non repudiation –Requires that neither sender nor the receiver of message should be able to deny the transmission.

• *Access control* – Access to information may be controlled by or for the target system.

• *Availability* – Requires that information be available to authorized parties when needed.

1.3 Classification of Cryptography

1. Symmetric key cryptography–

It is also called secret-key or shared key cryptography. In Symmetric cryptography, same key is used for encryption and decryption. Key plays an important role in cryptography. The key should be distributed before transmission between two parties. This type of cryptographic technique is required because it provides faster service without using many resources [2]. The strength of symmetric key encryption depends on the size of the key. Data can be easily decrypted if a weak key is used in the algorithm. There are various symmetric key algorithms such as DES, 3DES or TDES, AES, Blowfish[3]

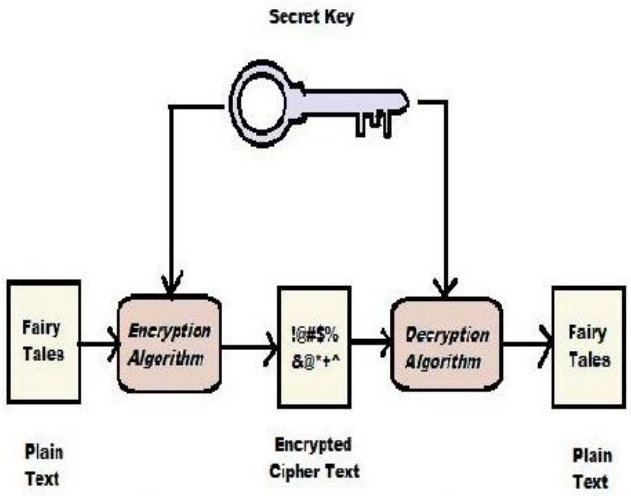


Fig-2: Symmetric key cryptography

2. Asymmetric key cryptography –

It is known as public key cryptography. In asymmetric key encryption, two different keys are used for encryption and decryption - public and private key. The public key of the receiver is used to encrypt the plain text and only the authorized person can be able to decrypt the cipher text through his own private key. Private key is kept secret. This method is more convenient and provides better authentication as the privacy remains intact [2]. There are various symmetric key algorithms such as RSA, Diffie Hellman Key Exchange Algorithm, ECC (Elliptical Curve Cryptography) and Digital Signature.

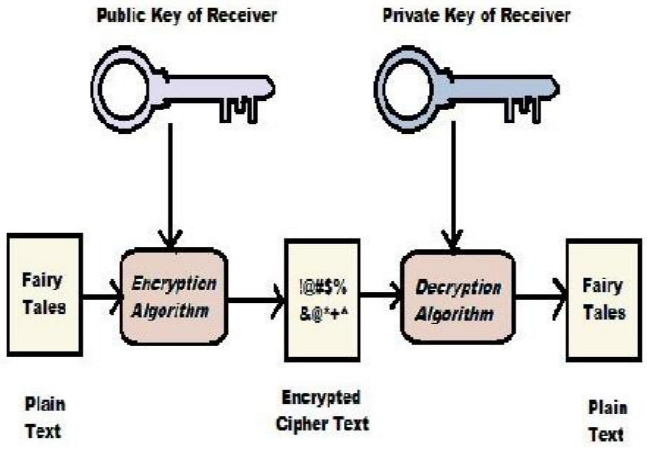


Fig-3: Asymmetric key cryptography

2. COMPARISON STUDY ON GENERAL SYMMETRIC KEY ALGORITHMS

The symmetric key cryptography are classified below-

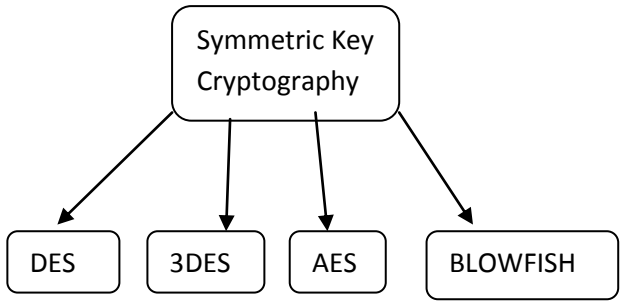


Fig-4: Symmetric Key Algorithms Classification

Table- 1: Comparison Table For Different Symmetric Key Algorithms

	Symmetric Encryption Algorithms			
	DES	*TDES*	*AES*	*BLOWFISH*
Block Size	64 bit	64 bit	128 bit	64 bit
Key size	56 bit	168 bit	128,192, 256 bit	32-448 bit
Created By	IBM in 1975	IBM in 1978	Joan Daeman in 1998	Bruce Schneier in 1998
Algorithm Structure	Fiestel Network	Fiestel Network	Substitution Permutation Network	Fiestel Network
Rounds	16	48	9,11,13	16
Attacks	Brute Force Attack	Theoretically possible	Side Channel Attacks	Not Yet

3. COMPARISON STUDY ON GENERAL ASYMMETRIC KEY ALGORITHMS

Asymmetric key cryptography are classified below.

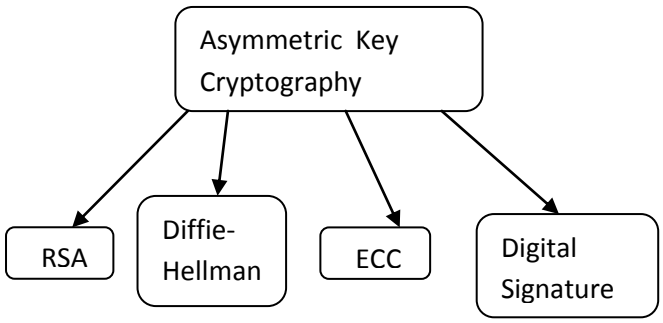


Fig-5: Classification of Asymmetric Key Algorithms

Table-2: Comparison Table For Different Asymmetric Key Algorithm

Method	Rivest-Shamir-Adleman (RSA)
Features	General form is (d, e) where d represents the private key and e represents the public key. Both encryption and decryption uses the same function [4]
Advantages	It is difficult to produce the private key from the public key and modulus, thus it is highly secure. Computing the reverse of e is very difficult for the attackers [5].
Downsides	Complexity of generating the key [6] . The process is quite slow. It has not been proved that it is equivalent to the factorization method and factorising a large number is very difficult.
Security Solutions	Key length should be larger than 1024 bits [5]
Method	**Diffile Hellman Algorithm**
Features	It is based on sharing the secret cryptographic key. This key is used for both encryption and decryption purposes. It relies on hardness of the discrete logarithms
Advantages	As the symmetric key is of very short length (256 bits), the algorithm is quite fast [7] .
Downsides	The longer the symmetric key is used the more attacks it will face More vulnerable to **Man In The Middle Attacks** [8]
Security Solutions	Frequent key changing is essential. Development of Station-to-Station protocol defeats Man in the Middle attacks. The development **Biometric Authentication** is a solution to the attacks.

Method	Elliptical Curve Cryptography (ECC)
Features	It computes the keys through elliptic curve equations [9].
Advantages	It can yield security using a 164 bit key and is more advantageous than RSA and Diffie Hellman algorithms [10]. It consumes less power and provides better utilities to batteries.
Downsides	It increases the size of encrypted message and is more complex and difficult to implement, compared to RSA [11].
Security Solutions	Introduction of Elliptic Curve Digital Signature Algorithm (ECDSA) [12].The Authenticated key agreement protocol, ECMQV protects against Man-in-the-Middle attacks.
Method	Digital Signature Algorithm (DSA)
Features	It consists of a pair of large numbers, computed based on some algorithms to authenticate data [13]. The signatures are generated through private keys and are verified using public keys.
Advantages	It is very fast and provides non-repudiation and authenticity [14]. It secures the data against various attacks like Man-in-the-Middle attacks and is more advantageous than other asymmetric key algorithms.
Downsides	Digital signatures have short life span. They are not compatible with each other and thus complicate sharing [14].
Security Solutions	Verification software is necessary. Digital certificates should be bought from trusted authorities.

4. COMPARISON STUDY OF NEWLY PROPOSED SYMMETRIC KEY ALGORITHMS

Table-3: Comparison Table For The Newly Proposed Symmetric Key Algorithms

Method	Algorithm against DPA attacks for both chips and Logic Circuits [15]
Characteristics	The model equations are first compared to that of CPA and then applied to AES and DES algorithms.
Advantages	It increases the robustness against the DPA attacks.
Pitfalls	Increasing the bus width will increase the number of keys. Hence, detection of correct key becomes difficult.
Implementations	Crypto chips and static logic circuits.
Method	Instruction Set Extensions for Symmetric Key algorithms
Characteristics	It includes the codesign of hardware and software paradigms to achieve physical security, flexibility, portability and better performance with hardware implementations.
Advantages	It reduces execution time, program code size and increases the throughput.
Pitfalls	Embedded systems without any modified processor increases overhead, data transfer latency and other complexities.
Implementations	Medical databases, e-mails, e-commerce, e-banking, etc.
Method	Parallel hardware architecture for AES-GCM algorithm[15]
Characteristics	It optimizes a number of logic gates and then compares the performance of S-Boxes with ASIC 65 nm CMOS technology.
Advantages	It provides both authenticity and confidentiality simultaneously for sensitive data.
Pitfalls	If the area effort increases, the overhead delay increases. If the critical path delay increases, the sub pipelining of the system cannot increase its frequency.
Implementations	Various hardware and software
Method	Fast encryption algorithm for multimedia (FEA-M) [16]

Characteristics	It uses resynchronization process for chosen and known plain text attacks.
Advantages	It provides an efficient alternative against breakability of FEA-M to various attacks.
Pitfalls	The process has weakness in the algebraic structures used.
Implementations	Has various multimedia applications
Method	Key transfer protocol for secret sharing applications [17]
Characteristics	It uses various threshold and secret sharing schemes for key exchange. It highlights both message authentication and conditional access.
Advantages	It allows the generation of different keys for the different set of receivers. It employs minimum computational requirements and does not depend on any mathematical assumptions.
Pitfalls	The process consumes much time.
Implementations	Satellite, internet, cable networks, etc.
Method	Rekeying architecture based on Tree Parity Machine
Characteristics	It uses TDMA with a single TPM unit. It implements both FPGA and ASIC realization using VHDL.
Advantages	It is cost effective, consumes less time with a limited bandwidth and overhead.
Pitfalls	Key lifetime is short. It reduces the storage area by increasing the cycles for generating the output bit.
Implementations	Embedded system environments.
Method	Instruction Level distributed Processor (COBRA)
Characteristics	It provides flexibility through reconfiguration. It maps and implements the algorithms using COBRA assembly language. Data is gathered using cycle counts.
Advantages	It provides both high speed processing and security. It provides an efficient implementation of a variety of block ciphers and can achieve a through of 622 Mbps.
Pitfalls	The block ciphers to be tested should be of varying efficiency and performance.
Implementations	Various network encryption implementations like ATM.
Method	Compression and Encryption scheme based on arithmetic coding and coupled chaotic systems [18]
Characteristics	It depends on zero-order arithmetic coding using bit streams generated by CCS PRBG. Algorithms are tested using text files.
Advantages	It is highly secure and is not vulnerable to attacks against arithmetic coding and plain texts.
Pitfalls	The zeroth order suffers about 6% over other techniques.
Implementations	Various ad hoc networks.
Method	Operation Centred approach of fault detection [19]
Characteristics	It enumerates the arithmetic and logical operations and then analyses the efficiency and hardware complexity using 11 symmetric ciphers.
Advantages	It can perform the analysis even if the error propagation is non-linear. Detection coverage is 100%
Pitfalls	Analysis of multiple bit error is complicated.
Implementations	Ad Hoc networks, etc.
Method	Sharing Session Key component algorithm
Characteristics	Messages are protected through radio links and are clear for network operator. The algorithm operates so long the communication is disputed to endanger public safely.
Advantages	It improves symmetric key encryption technique by providing non-repudiation and end-to-end security to each individual in communication.
Pitfalls	Key Escrow Trust Organization cannot recover the session key. It has finite computing capacity and less power.
Implementations	Digital Mobile communications, E-commerce

Method	Symmetric key encryption algorithm based on 2-d geometry [20]
Characteristics	It includes both the properties of circle and circle centred angles. It provides high confidentiality with less computational complexity.
Advantages	In every steps of encryption, it produces fixed size messages.
Pitfalls	Floating point operations limit the size of block to encode. Hardware implementation is tricky.
Implementations	E-commerce, banking, stock trading, etc.
Method	Method of Digital Signature based on combined symmetric key algorithm
Characteristics	It depends on both symmetric and hardware technology. It uses timestamps as a factor of such symmetric key algorithms.
Advantages	The key is time variant and maintenance free. It deciphers faster and has a simple key management compared to asymmetric digital signature algorithms.
Pitfalls	The process is slight lengthy.
Implementations	Various transactions like e-commerce, etc
Method	Hill-Shift-XOR encryption technique for image encryption
Characteristics	Encryption is performed using block wise XOR operations. It can operate in color, gray scale and binary images.
Advantages	It is reliable where cryptanalysis is quite difficult. It is robust.
Pitfalls	The technique is relatively slow.
Implementations	Digital data protection, copy protection, etc.

Method	NJJSAA Symmetric key algorithm [21]
Characteristics	The process performs key exchange and XOR operations for both encryption and decryption.
Advantages	It is better than other general cryptographic algorithms. It can encrypt both large and small files.
Pitfalls	The process is slight lengthy.
Implementations	Government sectors, banks, database encryption, etc.
Method	DJMNA Symmetric key algorithm
Characteristics	It combines both MGVC and DJSA methods. The order of these algorithms depends on the random matrices developed during the process.
Advantages	The encrypted message is very hard to decrypt using any Brute Force attack.
Pitfalls	The process is complex and lengthy.
Implementations	Password encryption, mobile network, ATM network, etc.
Method	Symmetric key based RFID authentication protocol
Characteristics	It implements three protocols that use same block cipher by implementing same RF based hardware.
Advantages	This protocol improves the RFID system by providing security against various attacks at low computational cost.
Pitfalls	The process is lengthy.
Implementations	Communication networks, business houses, etc.
Method	Wireless Secret key generation algorithm in multiuser networks [22]
Characteristics	It works in multiuser networks and checks how such diversity affects secret key randomness.
Advantages	It increases the randomness performance and reduces the execution time.
Pitfalls	Update of secret key is necessary for proper security.
Implementations	Various wireless communication networks.

5. COMPARISON STUDY OF NEWLY PROPOSED ASYMMETRIC KEY ALGORITHMS

Table-4: Comparison Table For The Newly Proposed Asymmetric Key Algorithms

Method	Hardware/software codesign of ECC for Resource constrained applications [41]
Characteristics	It helps in binary field multiplication in software. It also offers instruction set extensions and presented a coprocessor for binary multiplication.
Advantages	It is highly efficient in terms of performance and area.
Pitfalls	Nothing has been mentioned about power consumption.
Implementations	Brand protections, etc.
Method	Prime Number Generation[24]
Characteristics	Prime numbers are generated randomly from a large series using the divisibility tests.
Advantages	Scrambled messages using two prime factors become difficult to break. So, data remains highly secured.
Pitfalls	The bit length of the prime numbers should be pre determined. Generating big prime numbers is quite difficult.
Implementations	Money transfer, business transactions, diplomatic communications, books, audio, video, etc.
Method	Image security through asymmetric watermarking algorithm
Characteristics	Embedding and detection are done separately using private and public key respectively. It is based on linear algebra.
Advantages	This algorithm is highly efficient as it provides a double layer security level for protecting digital data. It is simple and saves the computational cost.
Pitfalls	If a particular integer is big then the watermark is not detected to the original encrypted images.
Implementations	Copy protection frameworks
Method	Cryptanalysis using COPACOBANA[25]
Characteristics	It consists of 120 field programmable gate arrays. It can solve various computations without any mathematical breakthrough.
Advantages	It helps in faster RSA factorization and can secure ECC. It provides a cost effective service.
Pitfalls	To make the overall machine design cost effective, many small FPGA modules are designed. This requires extra space.
Implementations	Useful tool for parallel computational problems
Method	Generation of a multimode multiplier
Characteristics	The multimode multiplier consists of four phases and uses a series of right shifting and additions.
Advantages	The multimode multiplier consists of four phases and uses a series of right shifting and additions.
Pitfalls	The multimode multiplier wastes power if operated in AES mode. The power consumption is high.
Implementations	It can be applied to various polynomial fields and helps in matrix-vector multiplications.
Method	Master-key-encryption-based multiple group key management scheme (MKE-MGKM)
Characteristics	The MKE-MGKM is used to tackle various multicast groups existing in a single network.
Advantages	The MKE-MGKM is simple and requires less memory storage for the keys.
Pitfalls	Communication overhead is greater than storage overhead.
Implementations	Various broadcasting like TV and wireless mobile networks.
Method	Asymmetric Public Key Traitor Tracing Schemes [26]
Characteristics	It uses a multiplicative cyclic group of very big prime order and then it evaluates an oblivious polynomial.
Advantages	It traces the traitor, in digital content, responsible for the construction of pirate keys, ensuring non-repudiation.
Pitfalls	Broadcasting streams are quite expensive. There is a trade off between protection and

	content distribution.
Implementations	Various entertainment devices like TV.
Method	Feigenbaum encryption method of messages
Characteristics	It uses two pairs of asymmetric private keys. It makes use of a logistic difference equation.
Advantages	It, specially the double F-sequence coding, makes a better use of the encryption technique in the messages and can confuse the attacker who employs nearly the correct keys.
Pitfalls	The requirements are time consuming which cannot be satisfied by an efficient computer program.
Implementations	Various online communication mediums.
Method	Asymmetric DNA algorithm [27]
Characteristics	It encrypts the plain text using the existing biological information from the DNA public databases. It is implemented in BioJava and Matlab
Advantages	It does not require several iterations for derivation of keys and the keys can be retrieved. It is more reliable and powerful than OTP DNA algorithm.
Pitfalls	The process is lengthy and kills the execution time.
Implementations	Researches in DNA computations.
Method	Key assessment scheme for secure broadcasting [23]
Characteristics	The scheme employs ECC cryptographic algorithm. The number of encryption keys depends on the access control policies.
Advantages	It is highly efficient. Storage of decryption keys in tamper resistance device is easier.
Pitfalls	Security solutions especially in case of smart cards are not cleared.
Implementations	TV systems, electronic subscription, etc.

Method	Method for increasing security in RSA [28]
Characteristics	It eliminates the distribution of n large numbers whose factors become difficult to design using RSA algorithm.
Advantages	It protects the messages from the mathematical factorization attacks which the general RSA algorithm suffers from.
Pitfalls	It increases the time complexity.
Implementations	Various hardware and software
Method	Model based on Pretty Good Privacy (PGP) to secure E-Commerce through Asymmetric Key encryption technique
Characteristics	It implements the RSA algorithm for encryption or decryption purposes. It is based on PGP and dual signature method.
Advantages	It provides security issues at various levels like transaction level, reply attacks, mutual authentication, Network and transport level, etc.
Pitfalls	----------
Implementations	Biometric system, Internet banking, ATM machine, Key exchange and Digital signature, etc.
Method	Technique based on Elliptical Curve Cryptography (ECC) through the implementation of hidden generator point in WSNs
Characteristics	Digits are extended beyond two bits for representing k, where k is any integer in prime field as the ECC is represented as T=k*G where G are the points on elliptic curve. The 192-bit values are stored in a 24*8 array.
Advantages	It provides better security against the physical node capture and man in the middle attacks.
Pitfalls	The communication cost is high as it requires multiple computations.
Implementations	Various Wireless Sensor Networks

6. CONCLUSION AND FUTURE SCOPE

This paper gives the basic terms and concepts of cryptography and Complete basic comparison table among the popular Symmetric key algorithm and The Asymmetric key algorithms .A comparative study is very important for most researchers who want to know the most appropriate cryptographic techniques for use in their work.In Symmetric Key Cryptography, a single common key is for both encryption and decryption purposes. The sharing of this key becomes sometimes insecure. On the other part, Asymmetric Key Cryptography uses two different keys to prevent any unethical get entry to the data. The public key remains public and the private key is not shared. This method ensures higher security than the former. Furthermore, the use of Digital Signatures in case of Asymmetric Key Cryptography provides high information confidentiality and non-repudiation. Yet, Symmetric Key Cryptography has many well known applications due to its simplicity. To overcome the Man In The Middle Attacks or hacking case Biometric based cryptography will be the excellent choice because the biometric cryptography provide the Authentication. Biometric based authentication in Diffile Hellman Algorithm will reduce the Man in the middle attack problem. In future the Biometric based cryptography will give the new direction in for authentication and data security.

REFERENCES

[1] O.P Verma, RituAgarwal, DhirajDafouti and ShobhaTyagi, "Peformance Analysis Of Data Encryption Algorithms", IEEE Delhi Technological University , India,2011.

[2] voices.yahoo.com/comparing-symmetricasymmetric-key-encryption-6329400.html

[3] DiaaSalama, Abdul. Elminaam, HatemMohamed,Abdul Kader and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", International Journal of Computer Science and Network Security,vol.8No.12, December 2008.

[4]www.cs.usfca.edu/~brooks/S04classes/cs480/lectures/algs.pdf

[5]www.encryptionanddecryption.com/algorithms/asymmetric_algorithms.html

[6]scialert.net/fulltext/?doi=itj.2013.1818.1824

[7] www.vocal.com/cryptography/tdes/

[8]home.cyber.ee/ahtbu/CDS2011/SandraNetsajevaSlides.doc

[9]searchsecurity.techtarget.com/definition/elliptical-curve-cryptography

[10]William Stallings, "Cryptography and Network Security principles and practices ", fifth Edition, Pearson Education, 2003

[11]www.ehow.com/info_12226350_advantagesdisadvantages-elliptic-curve-cryptographywireless security.html

[12]vanilla47.com/PDFs/Cryptography/Miscellenea/Eliptic%20Curve%20Cryptography/A_tutorial_of_elliptic_curve_cryptography.pdf

[13]searchsecurity.techtarget.com/definition/Digital-Signature-Standard

[14] lerablog.org/technology/datasecurity/advantages-and-disadvantages-of-digitalsignatures

[15] Massimo Alioto, Massimo Poli, and SantinaRocchi, "Differential Power Analysis Attacks to Precharged Buses: A General Analysis for Symmetric-Key Cryptographic Algorithms", *IEEETransactions on Dependable and SecureComputing*, vol. 7, no. 3, pp. 226-239, July-Sept.2010, IEEE

[16] Miodrag J. Mihaljevic´, Ryuji Kohno,"Cryptanalysis of Fast Encryption Algorithm for Multimedia FEAM", *IEEE CommunicationsLetters*, vol. 6, no. 9, pp. 382-384, Sept. 2002,IEEE

[17] Ahmet M. Eskicioglu and Edward J. Delp, "A KEY TRANSPORT PROTOCOL BASED ON SECRET SHARING APPLICATIONS TO INFORMATION SECURITY", *IEEE Transactionson Consumer Electronics*, vol. 48, no. 4, pp. 816-824, Nov. 2002, IEEE

[18] Ranjan Bose and SaumitrPathak, "A Novel Compression and Encryption Scheme Using Variable Model Arithmetic Coding and Coupled Chaotic System", *IEEE Transactions on Circuitsand Systems—I: Regular Papers*, vol. 53, no. 4, pp. 848-857, April 2006, IEEE

[19] Luca Breveglieri, Israel Koren, and Paolo Maistri, "An Operation-Centered Approach to Fault Detection in Symmetric Cryptography Ciphers", *IEEE Transactions on Computers*, vol. 56, no. 5, pp. 635-649, May 2007, IEEE

[20] Mohammad JabedMorshedChowdhury and Tapas Pal, "A New Symmetric Key Encryption Algorithm based on 2-d Geometry", *2009International Conference on Electronic ComputerTechnology*, pp. 541-544, IEEE

[21] NeerajKhanna, JoyshreeNath, Joel James, AmlanChakrabarti, SayantanChakraborty, and AsokeNath, "New Symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm", *2011 International Conference onCommunication Systems and NetworkTechnologies*, pp. 125-130, IEEE

[22] SeonYeobBaek and Jongwook Park, "A Study on Wireless Secret Key Randomness in Multiuser Networks", *ICTC 2013*, pp. 1048-1052,IEEE

[23] WafaElmannai, KhaledElleithy, VarunPande, and ElhamGeddeda, "Quantum Security using Property of a Quantum Wave Function",IEEE

[24] ArunKejariwal, " Cryptic primes", *IEEE Potentials*, pp. 43-45, Feb./Mar. 2004, IEEE

[25] Tim Gu¨neysu, Timo Kasper, Martin Novotn_y, ChristofPaar, and Andy Rupp, "Cryptanalysis with COPACOBANA", *IEEE Transactions onComputers*, vol. 57, no. 11, pp. 1498-1513, Nov.2008, IEEE

[26] AggelosKiayias and Moti Yung, "Breaking a Repairing Asymmetric Public-Key Traitor Tracing", pp.1-16, IEEE

[27] RaduTerec, Mircea-Florin Vaida, LenutaAlboaie, and LigiaChiorean, "DNA Security using Symmetric and Asymmetric Cryptography", *TheSociety of Digital Information and WirelessCommunications*, vol-1, no-1, pp. 34-51, 2011, IEEE

[28] RohitMinni, KaushalSultania, Saurabh Mishra, and Prof Durai Raj Vincent, "An Algorithm to Enhance Security in RSA", *4thICCCNT 2013*, pp. 1-4, IEEE